コンテンツポイズニング攻撃の影響分析

Investigating Impact of Content Poisoning Attack

工藤 多空飛　　上山 憲昭
Takuto Kudo　　Noriaki Kamiyama
福岡大学 工学部 電子情報工学科
Faculty of Engineering, Fukuoka University

1. はじめに

コンテンツの名称でデータ通信を行い，コンテンツ配信を効率的に行うネットワークアーキテクチャとして情報指向ネットワーク (ICN: information-centric networking) が注目を集めている．しかし，悪意を持ったユーザが不当なコンテンツをネットワークに展開することでキャッシュの効果を低下させるコンテンツポイゾニング攻撃 (CPA: content poisoning attack) の問題が指摘されている [1]．CPA は，コンテンツと紐づいた公開鍵から生成されたディジタル署名と一致する偽のコンテンツをキャッシュ(CS: content store) に注入する fake 型と，ディジタル署名と一致しない無意味なコンテンツを CS に注入する corrupted 型の 2 つに大別される．CPA に対する対処法を確立するには，CPA がネットワークの性能に与える影響を明らかにする必要があるが，既存研究は限定された CPA 方式を想定しており，その多くが小規模なネットワークトポロジや攻撃者の位置で評価を行っており，汚染コンテンツ数や汚染ノードなどが CPA の脅威に与える影響が明らかにされていない [1]．そこで本稿では fake 型の CPA を想定し，大規模なネットワークトポロジで様々な攻撃者の位置で評価を多面的に行うことで，様々な要素が CPA の効果に与える影響を分析し，CPA の脅威を明らかにする．

2. コンテンツポイズニング攻撃

CPA の fake 型はその攻撃の性質から 2 つに分類される．攻撃者が独自に作成した fake コンテンツを結託した Client から要求することで CS に注入する独自 fake 型と，実在するコンテンツの fake コンテンツを正常な Client からの要求時に配信することで CS に注入する詐称 fake 型が考えられる．

独自 fake 型では，攻撃者が独自に作成した fake コンテンツにアクセスするのは攻撃者と結託した Client だけである．したがって正常で高名なコンテンツと比較して要求数が圧倒的に少なく，ルータの CS に注入できても一時的であるため効果が小さいことが予想される．

詐称 fake 型では，攻撃者のコンテンツに Client からの要求 (Interest) が転送されるよう FIB が設定される．実在する高人気コンテンツの fake コンテンツであるためアクセス数が非常に多く，攻撃の影響が非常に大きいことが予想される．正当な Publisher の公開鍵を管理している CA の職員と結託するなど，公開鍵を攻撃者の公開鍵に書き換えるなどすることで本タイプの攻撃が可能である．正当な Publisher の公開鍵を乗っ取って書き換える結果，攻撃者のコンテンツの方が正当化される．

3. 性能評価

CPA の fake 型の影響について計算機シミュレーションにより分析する．CAIDA で公開されている米国の商用 ISP のバックボーンネットワークトポロジのうち，ノード間の平均ホップ距離が小さくハブノードを経由することで少ないホップ長で他のノードに到着可能な Allegiance Telecom と，ノード間の平均ホップ距離が大きく他のノードに到着するには多数の中継ノードを経由する必要のある At Home Network の 2 つを評価に用いる．fake コンテンツは各ネットワークトポロジの最西端の 1 ノードに配置し，そのノードからホップ距離が最も大きい 1 ノードに結託ユーザを配置する．キャッシュ方式は経路上のすべてのルータでキャッシュを行う AllChace，配信要求ルータでのみキャッシュを行う EdgeCache，配信ルータの 1 ホップ下流ルータでキャッシュを行う Leave Copy Down(LCD)[2] の 3 種類を想定し，全てのキャッシュ方式においてキャッシュ置換法としては LRU を用いる．コンテンツ数 $M = 10,000$ に対しキャッシュサイズは 100 とし，1,000 秒間シミュレーションを行う．正常ユーザはパラメタ $\theta = 0.6$ の Zipf 分布に従いランダムに選択したコンテンツを要求する．

3.1. 独自 fake 型

独自 fake 型における結託ユーザは fake コンテンツのみをランダムに要求する．結託ユーザの数は一人を想定し，fake コンテンツは 10 個作成し，fake コンテンツのオリジナルの位置は結託ユーザから最も離れたノードに配置する．結託ユーザの要求比率は全要求比率に対して 0.01%から 10%まで変化させる

図 1 に独自 fake 型におけるキャッシュ方式 3 つに対し，結託ユーザの要求比率を変化させたときの，キャッシュから配信されたコンテンツの中で正常コンテンツの占める割合をプロットする．fake コンテンツへの要求は結託ユーザのみが行うため要求比率が低いときは攻撃の影響はほとんどない．結託ユーザの要求比率が 1%を超えたあたりから攻撃の影響が見られる．両ネットワークトポロジにおいて AllCache の場合の影響が大きく，(b) に示すようにハブノードが存在するネットワークトポロジにおいては EdgeCache の場合も影響も大きい．これはこれらのキャッシュ方式を用いた場合はネットワーク上の広範囲に fake コンテンツが展開されやすいためと思われる．

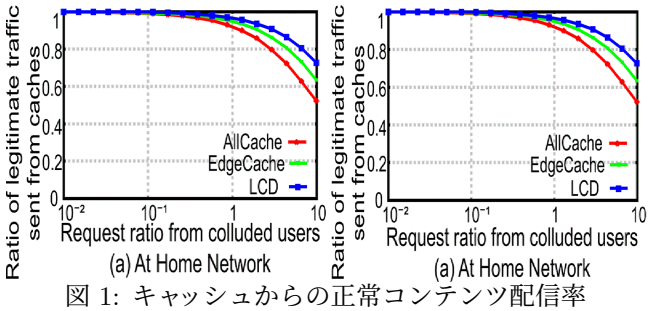

図 1: キャッシュからの正常コンテンツ配信率

3.2. 詐称 fake 型

詐称 fake 型における詐称コンテンツはコンテンツ人気度 1 位のものから x 位のものを対象とする．図 2 に詐称 fake 型におけるキャッシュ方式 3 つに対し，fake コンテンツ数 x を変化させたときのキャッシュヒット率をプロットする．ただしキャッシュヒット率は正常コンテンツの配信の中でキャッシュから配信された配信の割合と定義する．要求頻度の高いコンテンツを fake とするため影響が大きく，上位 100 位のコンテンツまでの fake コンテンツを作成することでキャッシュヒット率はどのキャッシュ方式においても半減している．両ネットワークトポロジにおいて AllCache と EdgeCache への影響は非常に大きく，(b) に示すようにハブノードが存在するネットワークトポロジにおいては EdgeCache に与える影響が特に大きい．

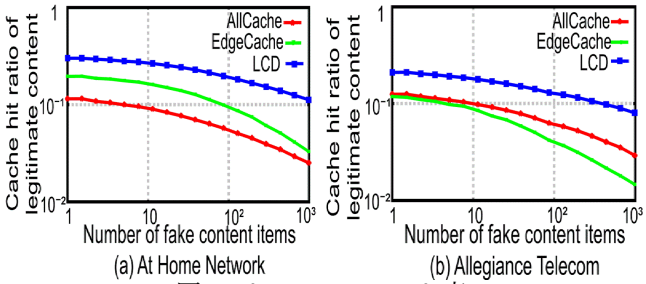

図 2: キャッシュヒット率

謝辞　本研究成果は JSPS 科研費 18K11283 の助成を受けたものである．ここに記して謝意を表す．

参考文献

[1] T. Nguyen, et al., Content Poisoning in Named Data Networking: Comprehensive Characterization of real Deployment. 2017 IFIP/IEEE Symposium on Integrated Network and Service Management(IM), pp.72-80, 2017.
[2] N. Laoutaris, H. Che, and I. Stavrakakis, “The LCD interconnection of LRU caches and its analysis,” Elsevier Performance Evaluation, Vol. 63, Issue 7, pp. 609-634, July 2006.